PROJECT-X1 xx1 Design Analysis Report

July 2004

Table of Contents

Tables

1 Executive Summary

The Independent Verification & Validation (IV&V) Team has completed an analysis of the Command and Data Handling (C&DH) Flight Software design for the PROJECT-X1 Project. The purpose of this analysis was to ensure the design properly accommodates the C&DH requirements and provides a sound foundation for subsequent implementation and verification activities. Findings and conclusions are summarized below and additional detail for each is provided in Section 4.

Significant findings resulting from analysis of the C&DH Flight Software Design include:

- Overall, the C&DH design is mature and of sufficiently high quality to ensure system needs will be met. A detailed comparison of the operational needs relative to the proposed C&DH design has not yet been analyzed, as the Concept of Operations has not yet been made available. However, due to the significant reuse from prior NASA Center X projects, it is felt that the PROJECT-X1 Project has a solid base from which operational concepts can be planned. IV&V has identified a small number of concerns in terms of elements missing from the design and elements with insufficient detail provided in the design. These issues are being tracked to closure in the IV&V Project Issue Tracking System (PITS).
- The PROJECT-X1 software development process does not provide for the creation of formal design documentation. Rather, design information is captured in the presentation charts developed in support of the Preliminary Design Review (PDR) and Critical Design Review (CDR). IV&V does not feel that review charts serve as a proper foundation for documenting the design of software that must be maintained for an extended mission lifetime. The generation of formal design documentation is fundamental to the software development process and should not be bypassed. Additionally, IV&V does not believe the design elements comprising each of the 23 C&DH packages are adequately documented within the review charts, i.e. the charts provide a good overview but do not suffice for detailed design. This can introduce risk to the successful implementation and long-term maintenance of the software.
- IV&V believes that the vast majority of requirements have been accounted for in the C&DH design, with 98% of the C&DH requirements having been addressed in the design. In some cases, the nature of the design documentation is such that it was not readily obvious that an item is present in the design, however leeway was given to all but the most difficult to find requirements; 15 requirements of the nearly 400 total requirements.
- Relatively few changes have been introduced during the design phase; however, a potential for more change exists as the development enters implementation, due to the 23 Action Items and Recommendations introduced at the January C&DH CDR. This introduces moderate risk that could affect the timely verification and delivery of the C&DH software.
- No testability issues with the design were identified, although test schedule margin is a concern.

- No problems with regard to data flow, control flow and moding/sequencing, were identified. However, a significant amount of data analysis has been deferred to the start of code analysis.
- Hardware resource allocation estimates are relatively mature due to the reuse aspects of the software. Currently only the XY Memory is over-subscribed based on NASA Center X XY Margin Requirements for CDR, with all other allocations within tolerance. The level of over-subscription for XY does not appear at this time to create a problem, although it is something that should be monitored especially in terms of future growth.
- In addition to the risks cited by the Project during the C&DH and Mission CDRs, the IV&V Team has identified other aspects of development that appear to add risk to the successful delivery and maintenance of C&DH software. They are:
    - Planning of formal acceptance testing for C&DH software is beginning very late in the development lifecycle.
    - S/C1 software milestone reviews may be inadequate for evaluating the quality of the software products and determining the readiness of the team to proceed into the next development phase.
    - Some risk to the process has been introduced by the late availability of the Software Development Plan (SDP) and the Software Quality Assurance Plan (SQAP). IV&V does not consider this to be a significant problem because it appears the Project has been following the processes described in the SDP all along. IV&V does not currently have access to the SQAP and cannot comment on whether those policies are being adhered to.
    - The Project does not have a well defined process to determine what code is subject to formal reviews. The IV&V Team believes the risk of inadequate code review is minimal, but will monitor the breadth and quality of the upcoming reviews.
    - There is some risk to the C&DH software due to the amount of work and coordination remaining for the Autonomy functionality.

  IV&V believes that these risks combine to pose a moderate to significant threat to the timely development and verification of the C&DH software.

2 Analysis Scope

The purpose of this report is to describe the analysis methodology, findings and recommendations resulting from IV&V analysis of the C&DH design for the PROJECT-X1.

The documents identified in Table 2-1 were reviewed during the course of this analysis.

Document Title	Document Number	Date
C&DH PDR Presentation Charts	-	xx/xx/xx
C&DH CDR Presentation Charts	-	-
C&DH Software Command xxx	-	xx/xx/xx
-	-	-
[REMOVED]		

Table 2-1 – Analysis Documentation

The documents identified in Table 2-2 were referenced during the course of this analysis.

Document Title	Document Number	Date
C&DH FSW Requirements	-	xx/xx/xx
PROJECT-X1 Software Development Plan	-	xx/xx/xx
NASA Center X XY Margin Requirements	-	-
NASA Software Documentation Standard	-	-
IEEE Recommended Practice for Software Design Descriptions	1016-1987	-
--	-	-
--	--	--
[REMOVED]		

Table 2-2 – Reference Documentation

3 Analysis Methodology

This section describes the approach and tools used to perform the design analysis activities provided for in the IV&V PROJECT-X1 Project Plan. The activities that are applicable to C&DH, based on the IV&V Analysis Levels (IALs), are shown in Table 3-1. This table also identifies the section in this report where the associated findings and conclusions are discussed.

Design Analysis Activity	Findings Section
Verify design documentation meets intended purpose, has appropriate detail and all necessary elements (design document quality)	4.1
Verify ability of design to meet system needs	4.2
Analyze database design	4.3
Analyze design testability and qualification requirements	-
Analyze design data flow, control flow, moding and sequencing	-
Analyze error/exception handling	-
Analyze development risks/mitigation plans	-
--	--
[REMOVED]	

Table 3-1 – Design Analysis Activities

Detailed design evaluation criteria are provided in the IV&V PROJECT-X1 Design Analysis Guidelines and will not be repeated here. However, it is appropriate to generally describe how the design analysis was performed. For activities that involve analysis of individual requirements as they relate to the design, the spreadsheet developed to capture requirements analysis findings/comments was updated to include the following items:

- Is the requirement represented in the design? (Yes/No)
- If Yes, implementing design package
- If Yes, PDR/CDR charts that reflect the requirement

This arrangement facilitates capture, organization and tracking of findings and comments. It also allows for the development of metrics (e.g. traceability errors, design issues, etc). The spreadsheet will be expanded as analysis proceeds into other development phases and will eventually collect all requirement specific information from parent traceability, through design, implementation and into the verification program.

The tools identified in Table 3-2 were used during the course of this analysis.

Tool	Use
DOORS	Used to extract Mission, S/C, and Application Requirements
PITS	Used to capture issues identified during this analysis
--	--

Table 3-2 – Analysis Tools

4 Analysis Findings and Conclusions

This section contains findings and conclusions resulting from each of the activities identified in Table 3-1.

4.1 Design Documentation Quality

Discussion

This analysis was performed to determine the acceptability of the C&DH design documentation. This evaluation was based on a comparison to IEEE standard 1016-1987 (*IEEE Recommended Practice for Software Design Descriptions*). In making this comparison, it was not assumed that the development organization has chosen to implement this standard. Rather, the standard was used as a reasonable gauge to measure against because it is widely accepted, well documented, and independent of design methodology.

In general, the IEEE standard considers design documentation acceptable if it provides the precise design information needed for planning, analysis, validation, and implementation of the software system. The design should represent a partitioning of the system into design entities and describe the important properties and relationships among those entities. A design entity is defined as an element of a design that is structurally and functionally distinct from other elements. The objective of establishing design entities is to divide the system into separate components that can be considered, implemented, changed and tested with minimal effect on other entities.

Each design entity should have a standard set of attributes. An attribute is a named characteristic or property of a design entity. A software design may be considered complete when all attributes have been specified for all design entities. The design entity attributes recommended by the IEEE standard are:

Attribute	Description
IDENTIFICATION	A unique name to identify the entity. All names should be connotative of the intended purpose of the named item and used consistently throughout the document.
TYPE	A description of the kind of entity. For example, process, module, algorithm, data store/file, class, etc.
PURPOSE	A description/rationale of why the entity exists in terms of satisfying specific functional and/or performance requirements. The objective of this attribute is to facilitate a trace to requirements.
FUNCTION	A statement of what the entity does. This attribute identifies transformations and control decisions applied by the entity. If it is a data entity, it states the type of data stored or transmitted.
SUBORDINATES	The identification of all entities composing this entity. The description may include both a logical and physical view. A logical view might identify subordinate classes or functions. A physical view would identify the files that package those classes or functions. The decomposition of an entity should occur in a manner that easily facilitates the comprehension of the entity. Typically this involves layers of abstraction, such that the volume of detail describing how the entity functions increases as one proceeds down through the layers.

Attribute	Description
DEPENDENCIES	A description of the relationships between this entity and other non-subordinate software design entities. It must identify all "uses" and "requires the presence of" relationships for this entity.
INTERFACE	A description of how other entities may interact with this entity. It must describe the methods of interaction and the rules governing those interactions. It should also define sources and frequency for all entity inputs along with range of inputs.
RESOURCES	A description of the elements used by the entity that are external to the design, e.g. Operating System (OS) services. In the preceding sentence, the word "design" is scoped to the design of the software system under development. Resources are the software and hardware that must be present and are accessed by, but external to, that scope.
PROCESSING	A description of the rules used by the entity to achieve its stated function. This attribute describes the algorithm or algorithms used to perform a specific task including contingencies (i.e., error and exception handling).
DATA	A description of data elements internal to the entity. The attribute shall describe the method of representation, initial values, use, semantics, format, and acceptable values of each element.

In addition to the description of design documentation provided in the IEEE standard, the C&DH design documentation was evaluated relative to the suggested content provided in the NASA Software Documentation Standard (NASA-STD-xxx). This standard provides for two design documents consisting of an architectural (preliminary) design and a detailed design.

The suggested table of contents for the architectural design document is:

1.0 INTRODUCTION
2.0 RELATED DOCUMENTATION
3.0 DESIGN APPROACH AND TRADEOFFS
4.0 ARCHITECTURAL DESIGN DESCRIPTION
5.0 EXTERNAL INTERFACE DESIGN
  5.1 Interface Design
  5.2 Interface Allocation
6.0 REQUIREMENTS ALLOCATION AND TRACEABILITY
7.0 PARTITIONING FOR INCREMENTAL DEVELOPMENT
8.0 ABBREVIATIONS AND ACRONYMS
9.0 GLOSSARY
10.0 NOTES
11.0 APPENDICES

The suggested table of contents for the detailed design document is:

1.0 INTRODUCTION
2.0 RELATED DOCUMENTATION
3.0 DETAILED DESIGN APPROACH AND TRADEOFFS
4.0 DETAILED DESIGN DESCRIPTION
  4.1 Compilation Unit Design and Traceability to Architectural Design
  4.2 Detailed Design of Compilation Units

5.0 EXTERNAL INTERFACE DETAILED DESIGN
5.1 Interface Allocation Design
5.2 Physical Interface Design
6.0 CODING AND IMPLEMENTATION NOTES
7.0 FIRMWARE SUPPORT MANUAL
8.0 ABBREVIATIONS AND ACRONYMS
9.0 GLOSSARY
10.0 NOTES
11.0 APPENDICES

Findings

- The PROJECT-X1 software development process does not provide for the creation of formal design documentation as described above. Rather, design information is captured in the presentation charts developed in support of the PDR and CDR. It is IV&V's understanding that the intention is to continually update these charts (even the PDR charts) to eventually reflect the as-built implementation. IV&V believes a Project of this size and complexity should document the software design in formally approved and configuration-managed documentation. Risk *xxx_xxx_007* documents this concern.
- Recognizing that formal design documentation is not being developed for the PROJECT-X1 C&DH software, the IV&V team considered the content of the design presentation charts relative to the previously described standards. In general, the charts are a good overview of the intended design and in some cases provide significant design detail. The design information is presented at a "package" level of detail, which is reflected for each of the 23 C&DH software packages. Design attributes associated with each package as represented in the diagrams are generally sufficient. For example, the charts contain adequate information about subordinates, dependencies, high-level interfaces, resources and basic processing flow of a given function. Data description, however, is generally insufficient in that the charts do not show all data usage.
- IV&V's primary concern relative to the design charts is that there is insufficient description of the design entities that comprise each package to fully evaluate the adequacy of the design. With only a few exceptions, these entities have no textual description of their purpose, function, basic processing and data usage/exchange to support a complete understanding of the diagrams supplied.

Conclusions

IV&V does not feel that review charts serve as a proper foundation for documenting the design of software that must be maintained for an extended mission lifetime of over xx years. The generation of formal design documentation is fundamental to the software development process and should not be bypassed. Additionally, IV&V does not believe the design entities comprising each of the 23 C&DH packages are adequately documented within the review charts. This introduces risk to the successful implementation and long-term maintenance of the software.

4.2 System Needs

Discussion

It follows that if the requirements have been determined to meet system needs and the design adequately represents the requirements, then the design should also meet system needs. Therefore, the determination as to whether system needs are being met by the proposed design is partially related to how well the design can be traced back to the requirements (this aspect of the analysis is discussed in Section 4.3).

In addition to simply tracing to the requirements, a design must be of sufficiently high quality if the resulting software is to meet system needs. For the purpose of this analysis, a high quality design is defined as being understandable, feasible, maintainable, evolvable, reliable and robust. To perform this analysis, the following types of questions were addressed:

- Is the design consistent with the objectives stated within the Concept of Operations Document?
- Does the design adequately support operational scenarios?
- Does each design entity support all of the mission aspects of the system (all devices, commands, silent periods, sleep periods, application processing)?
- Is process scheduling adequately described and suitable for the operating environment?
- Has a complete xxx been accomplished? Do the design entities support the required failure response?
- Has a hazard analysis been accomplished? Have specific hazards been allocated to software for control? Do the design entities support control of the allocated hazards?
- Does the design entity facilitate troubleshooting? Is failure information retained and made available via ground command?
- Do the design entities solve common problems in common ways? What is the mechanism for exception handling, storage management, overrun handling, telemetry collection, message passing, command handling, data sharing, initialization, time handling, mass storage access and resource sharing?
- Are there critical paths through the system for which end-to-end latency is important? Does the design adequately accommodate this latency?
- Have the functional, sequence and timing characteristics of the interfaces between design entities and between design entities and the external environment been described?
- Is the design sufficiently modular to provide for adequate maintainability?
- Do the design entities have high cohesion and low coupling?

This report does not comment when these questions were resolved in the affirmative and it can be assumed that the IV&V Team does not take issue with any aspect of the design that is not specifically addressed below. Note that in some cases, the nature of the documentation made it difficult to make an adequate determination. See Section 4.1 of this report for more detail regarding documentation concerns. Areas of concern and other comments relating to the design are described below in no particular order.

Findings

- The majority of the core design is reused from PROJECT-X2, where it underwent extensive planning and review. Specific control scenarios between the missions differ, but there appears to be significant commonality between how they are

commanded and controlled. As a result, the PROJECT-X1 Project enjoys significant benefit from this reuse. Several mission unique operational needs exist due to power constraints and the mission longevity. Many, if not most, of the core operational concepts have long since been thought out and the C&DH design appears to be capable of addressing them.

- As mentioned above, the proposed C&DH design appears to address the general operational needs for the PROJECT-X1 mission. However, a Concept of Operations document has not yet been provided to IV&V and consequently, an in-depth assessment of C&DH operational capability relative to the design cannot be performed. This analysis will be done once this document is released.
- As of this writing, design and operational concepts for Autonomy have yet to be completed. Because of the critical interaction between these two functions, there is risk to the C&DH software by proceeding with implementation prior to identification of all Autonomy concepts. IV&V recognizes that it is impractical to delay C&DH development until Autonomy matures, but this situation should be closely monitored to reduce the impact on the C&DH software due to late breaking Autonomy needs/requirements.
- A number of minor issues (approximately 17) regarding consistency and accuracy of the CDR design charts, xx Bus Specification and C&DH Command Documentation were noted during IV&V analysis with five submitted to the developer during the C&DH CDR. These issues do not reflect serious design problems but should be addressed before proceeding very far into implementation. An additional 23 issues identified after the CDR are presented later in this document.
- Finally, it does not appear that a Hazard Analysis has been performed by the Project to identify and mitigate the hazards that the S/C may face. Of particular interest to IV&V would be the hazards that are allocated to software for control.

Conclusions

Overall, the C&DH design is mature and of sufficiently high quality to ensure system needs will be met. A detailed comparison of the operational needs relative to the proposed C&DH design has not yet been made due to the lack of documentation; however, it is clear that the PROJECT-X1 Project benefits significantly from C&DH reuse from other missions. IV&V has identified a relatively small number of concerns with the C&DH design and documented these issues in PITS, where they are being tracked to closure.

4.3 Database Design

Discussion

Database analysis ensures that the database structure and access methods are compatible with the logical design. It was performed to ensure that common data and variable regions are used consistently between all calling routines, data integrity is enforced, no data or variable can be accidentally overwritten (e.g. by overflowing data tables) and that data typing and use are consistent throughout the program.

Findings

- Only general data usage information is provided in the C&DH design information, i.e. CDR charts. General data flow between package entities is shown in the package diagrams, but the details of this data exchange, e.g. specific parameters, format, table/queue size, frequency, etc., are not provided. Also, not all data store locations are shown on the design diagrams.

Conclusions

Given this lack of design detail, it was not possible to perform an in-depth database design analysis. This activity will be deferred until code analysis begins. At that point, it will be possible to determine directly from the code, the nature of data usage. This introduces a certain element of risk in that if there are data usage problems, they will not be discovered until after the start of implementation.

5 Summary of Issues and Risks Identified in Previous Reports

This section presents the status of issues and risks presented in the C&DH Requirements Analysis Technical Report that was delivered on xx/xx/xxxx. That report discussed IV&V analysis findings involving the C&DH requirements and contained several issues, risks and recommendations. Appendix C provides added details of those issues along with their current status.

The IV&V Team believes good progress has been made on the recommendations made in the previous report. Three of the six risks identified in that report have been closed. Of xx PITS issues, xx have been closed, x have actions taken and xx remain open. ..

[REMOVED]

6 Recommendations

Table 6-1 contains a list of recommendations based upon the findings discussed in this report.

#	Recommendation
1	Describe the plan and schedule to a sufficient level of detail to show how software design, implementation, and verification can be achieved per integration and test needs.
2	
	[REMOVED]

Table 6-1 – IV&V Recommendations

Appendix A: Issues

This appendix summarizes issues that were identified during C&DH design analysis.

XXX-TIM	Title	Issue
1001	Sufficiency of Design	There is insufficient description of the individual design entities to evaluate the adequacy of design as presented in the design presentation. For example, functions have no detailed description of their overall purpose, responsibilities and basic processing to support a complete understanding of the design/diagrams supplied. … Recommend reviewing detailed design …
1002	--	--
1003		
		[REMOVED]

Appendix B: Risks

This appendix summarizes C&DH related risks opened since the requirements analysis phase.

TIM	Title	Risk	Discussion
901	Late Start for Planning of Formal Software Acceptance Testing	It is IV&V's opinion that the spacecraft software ….	Project Response: …
902	--	--	--
--	--	--	--
	[REMOVED]		

Appendix C: Status of Previously Opened Issues and Risks

This appendix summarizes previously opened C&DH related issues and risks.

Status	Item	Discussion
Open	--	--
Closed	--	--
--	--	--
	[REMOVED]	

7 Acronyms

C&DH	Command and Data Handling
CDR	Critical Design Review
FMEA	Failure Modes and Effects Analysis
G&C	Guidance and Control
IAL	IV&V Analysis Level
ICD	Interface Control Document
IEEE	Institute of Electrical and Electronics Engineers
IV&V	Independent Verification and Validation
NASA	National Aeronautics and Space Administration
PDR	Preliminary Design Review
PITS	Project Issue Tracking System
SDP	Software Development Plan
SRR	Software Requirements Review
SRS	Software Requirements Specification
STD	Software Test Description
STP	Software Test Plan
TIM	Technical Issue Memorandum